IMPORTANT: Créez un nouveau document Word et enregistrez-le comme **VotreNom_Lab10.docx**. Il y aura 5 captures d'écran que vous devez coller dans ce document.

Exercice 1 – Installer OpenSSL

Dans cet exercice, vous allez apprendre comment Installer le logiciel OpenSSL pour générer des clés privées et publiques

1. Ouvrez **Microsoft Edge**. Allez sur le site :

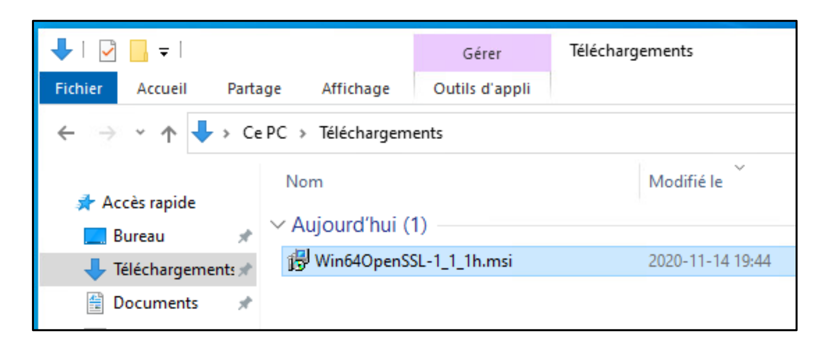
   https://slproweb.com/products/Win32OpenSSL.html

2. Allez au milieu de la page web, et cliquez sur **MSI** au-dessous du fichier **Win64 OpenSSL v1.1.1h** pour le télécharger.

Download Win32/Win64 OpenSSL today using the links below!

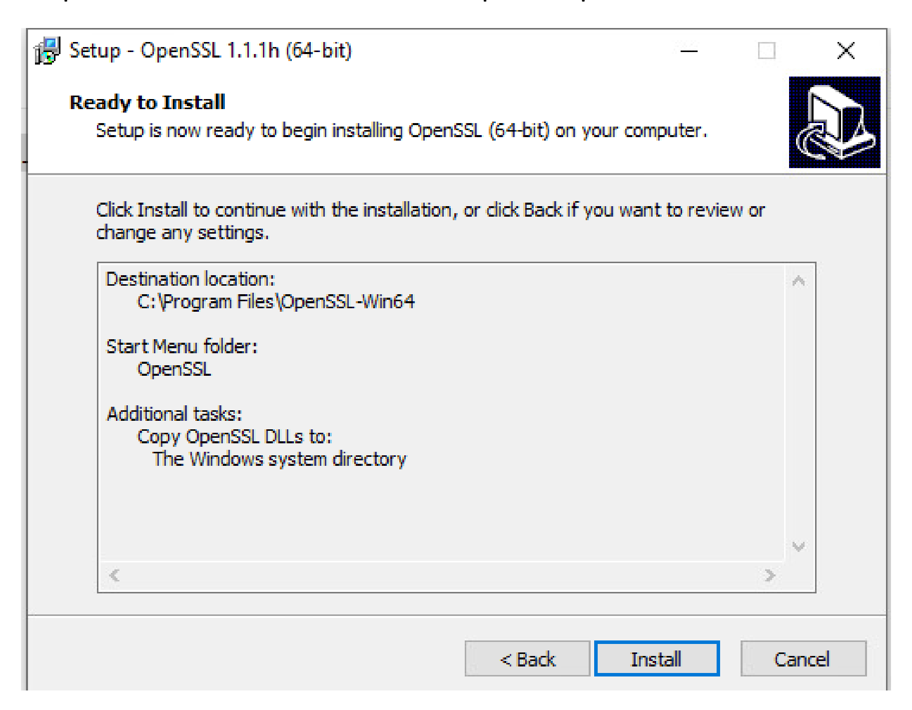
File	Type	Description
Win64 OpenSSL v1.1.1h Light EXE | MSI	3MB Installer	Installs the most commonly used ess build of OpenSSL and is subject to lo
Win64 OpenSSL v1.1.1h EXE | MSI	63MB Installer	Installs Win64 OpenSSL v1.1.1h (Re subject to local and state laws. More
Win32 OpenSSL v1.1.1h Light EXE | MSI	3MB Installer	Installs the most commonly used ess state laws. More information can be f
Win32 OpenSSL v1.1.1h EXE | MSI	54MB Installer	Installs Win32 OpenSSL v1.1.1h (On found in the legal agreement of the ir

3. Une fois téléchargé, allez dans le dossier **Téléchargement** et exécuter **Win64OpenSSL-1_1_1h.msi.**

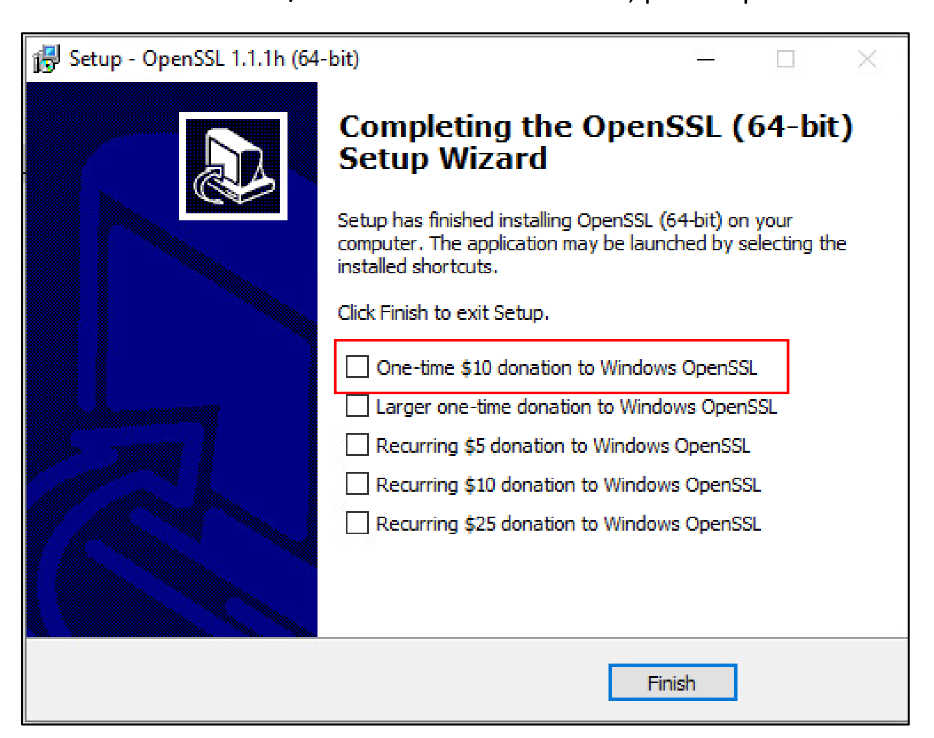


4. Cliquez sur **Oui** pour accepter.
5. Cochez **I accept the agreement** puis cliquez sur **Next.**

6. Cliquez sur **les trois Next** suivantes puis cliquez sur **Install.**



7. Décochez **One-time $10 donation to Windows**, puis cliquez sur **Finish.**

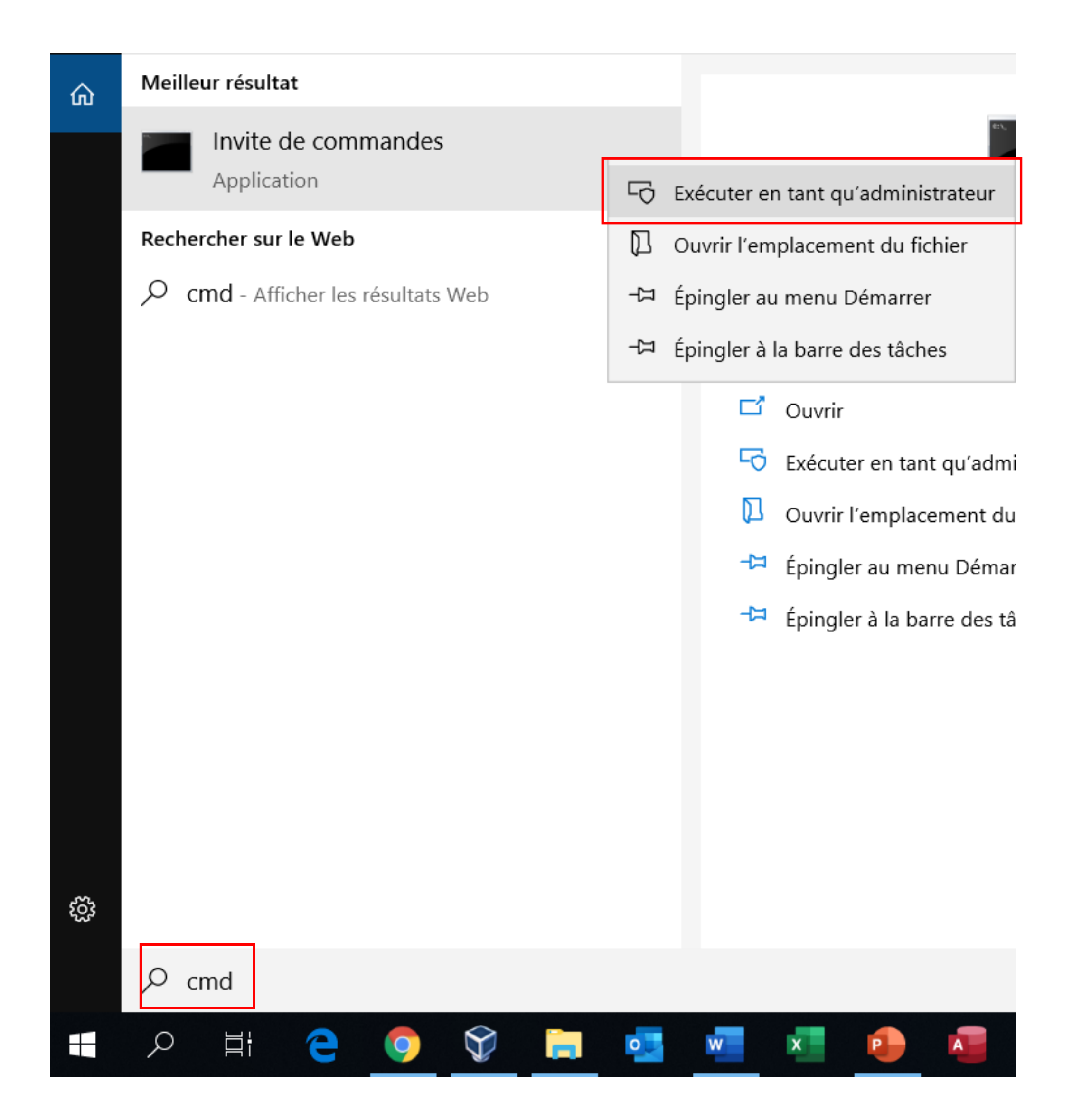


Exercice 2 – Création d'une clé privée et un certificat SSL

Dans cet exercice, vous allez apprendre comment utiliser OpenSSL pour générer une clé privée et un certificat SSL qui contient une clé publique

1. Ouvrez **l'invite de commandes** en mode **administrateur,** comme suit :

   Tapez **cmd** dans le bouton rechercher. Une fois **Invite de commandes** s'affiche, cliquez avec le bouton droit de la souris et sélectionnez **Exécuter en tant qu'administrateur.** Cliquez sur **Oui** pour accepter.



2. Changez de dossier pour aller dans le dossier qui contient le logiciel **OpenSSL :**

   cd C:\Program Files\OpenSSL-Win64\bin

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.18363.1198]
(c) Microsoft Corporation, 2019. Tous droits réservés.

C:\WINDOWS\system32>cd C:\Program Files\OpenSSL-Win64\bin

C:\Program Files\OpenSSL-Win64\bin>
```

3. Exécutez la commande **OpenSSL** :

   openssl

```
C:\Program Files\OpenSSL-Win64\bin>openssl
OpenSSL>
```

4. À ligne de commande **OpenSSL>**, vous allez taper la commande suivante, pour générer **une clé privée de 4096 bits**, en utilisant l'algorithme **RSA**, et vous allez nommer le fichier qui contient la clé **private.key.**

   genrsa -out private.key 4096

```
OpenSSL> genrsa -out private.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
..............................++++
............................................................++++
e is 65537 (0x010001)
OpenSSL>
```

5. Une clé privée de 4096 bits sera créée dans le fichier **private.key**.

6. À cette étape vous allez créer **un certificat numérique X509 (SSL)** qui :
   - Continuera **la clé publique** et autre information, comme le nom du pays de ce certificat, le nom du site web, l'adresse courriel de l'admin.
   - Une date d'expiration de **1826 jours (5 ans).**
   - Sera **signé par la clé privée** créée à l'étape précédente.
   - Le nom du certificat sera ***VotreNom*.crt**
7. Tapez la commande suivante, puis cliquez sur **Entrée**.

   req -new -x509 -days 1826 -key private.key -out *VotreNom*.crt

8. Puis entrez les informations encadrées en bleu là-dessous :

```
OpenSSL> req -new -x509 -days 1826 -key private.key -out tohme.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:QC
Locality Name (eg, city) []:Laval
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tohme
Organizational Unit Name (eg, section) []:703
Common Name (e.g. server FQDN or YOUR name) []:www.tohme.ca
Email Address []:admin@tohme.ca
OpenSSL>
```

IMPORTANT 1 : Prenez une capture d'écran de cette fenêtre ci-dessus et mettez-la dans le doc Word.

9. Une fois terminé, tapez **exit** pour sortir du OpenSSL et encore une fois **exit** pour fermer l'invite de commande.

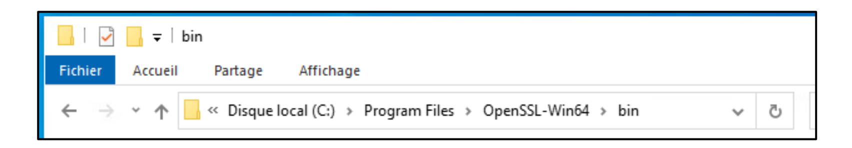
```
OpenSSL> exit

C:\Program Files\OpenSSL-Win64\bin>exit
```

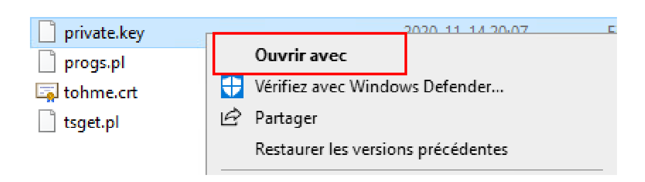
Exercice 3 – Visualiser la clé privée et le certificat

Dans cet exercice, vous allez apprendre comment visualiser la clé privée et le certificat qui contient la clé publique

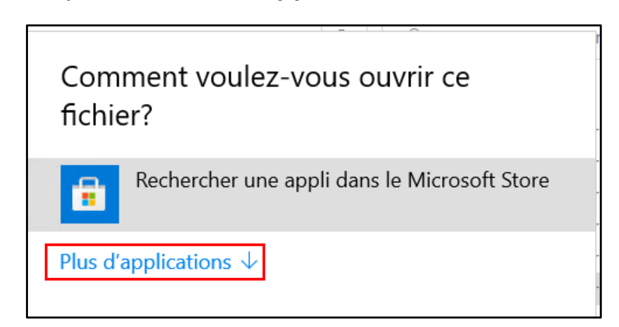
1. Allez dans le dossier **C:\Program Files\OpenSSL-Win64\bin**



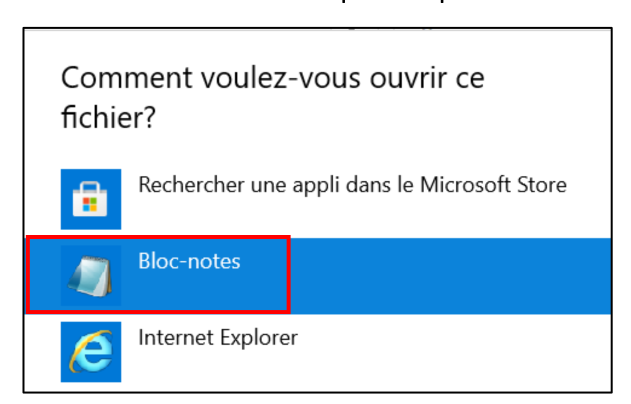
2. Cliquez avec le bouton droit sur le fichier **private.key** et sélectionnez **Ouvrir avec.**



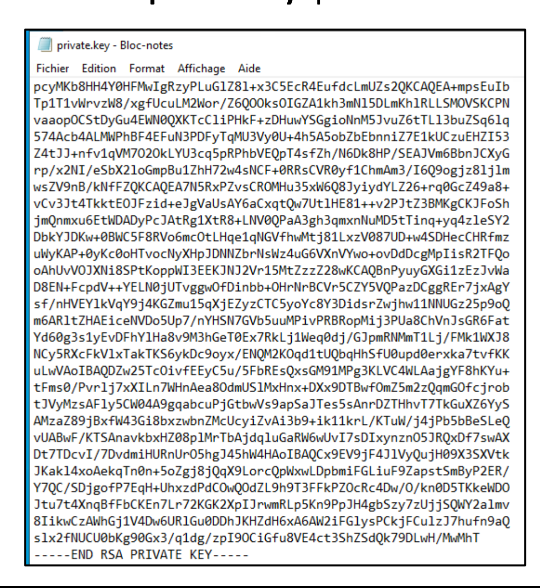
3. Cliquez sur **Plus d'applications**



4. Sélectionnez **Bloc-notes** puis cliquez sur **OK**.



5. Le fichier **private.key** qui contient **la clé privée** s'affiche comme suit :



IMPORTANT 2 : Prenez une capture d'écran de la clé privée et mettez-la dans le doc Word.

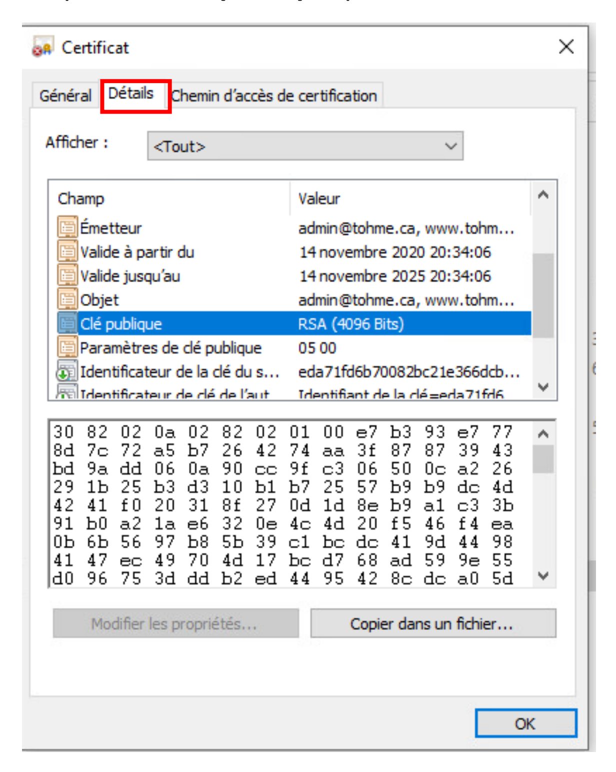
6. Fermez ce fichier et double cliquez sur le fichier ***VotreNom*.crt** pour ouvrir **le certificat**.



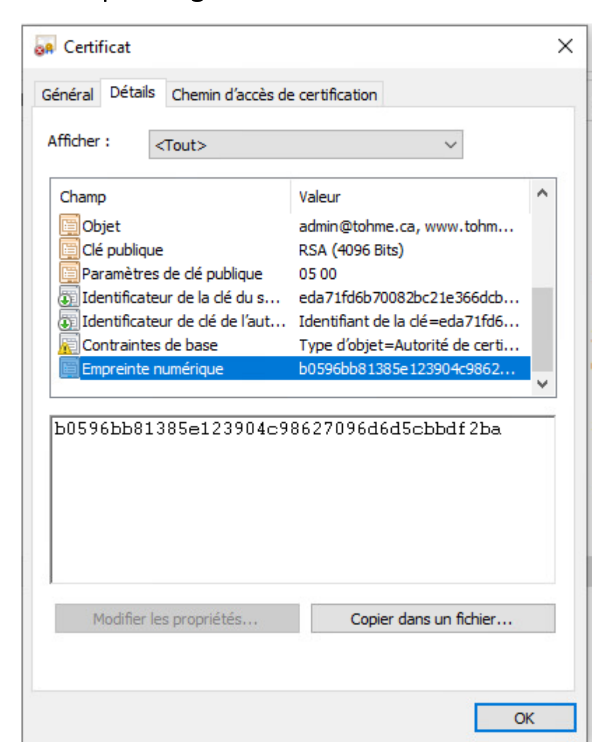
IMPORTANT 3 : Prenez une capture d'écran du certificat et mettez-la dans le doc Word.

7. Sous l'onglet **Général**, vous verrez une erreur, car ce certificat n'était pas approuvé par une **autorité de certification**. Vous verrez aussi le **nom de votre site** et **la date d'expiration de 5 ans**.

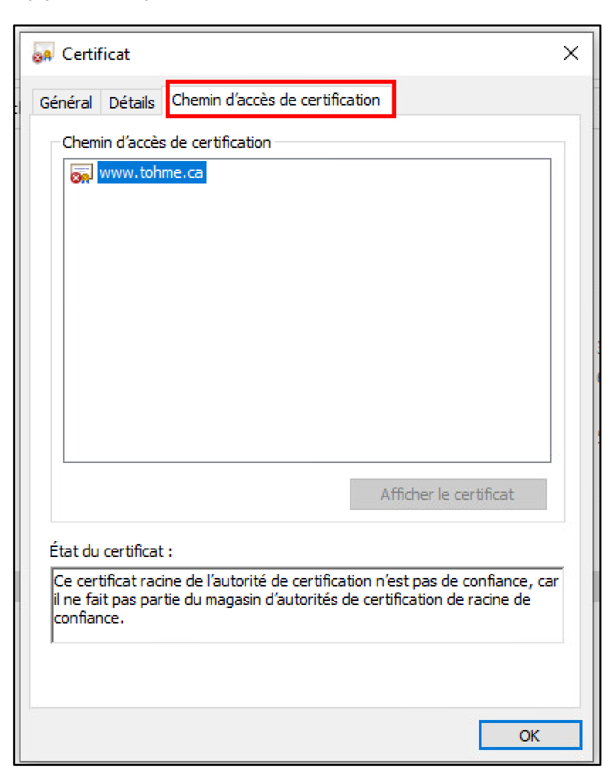
8. Cliquez sur l'onglet **Détails**, vous verrez l'adresse courriel de l'admin, la date d'expiration, **la clé publique** créée par l'algorithme RSA.
9. Cliquez sur **Clé publique** pour l'afficher.



10. Allez jusqu'à la fin de la liste, et cliquez sur **Empreinte numérique** pour voir la signature créée par l'algorithme **SHA-256**.



11. Cliquez sur l'onglet **Chemin d'accès de certification**, vous verrez que ce certificat ne peut pas être utilisé pour l'authentification, car vous l'avez créée manuellement et il n'était pas approuvé par un serveur d'autorité de certification de confiance connue par Windows.



12. Pour régler ce problème, nous allons **installer ce certificat dans le magasin de certificats de Windows 10** dans le dossier **Autorité de certificat racine.**

13. Allez à la page suivante pour voir comment installer un certificat.

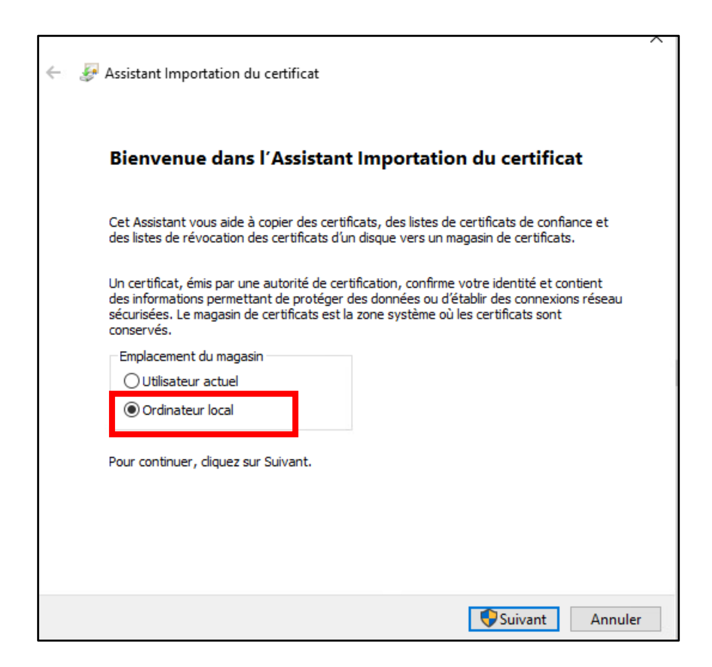
Exercice 4 – Installer un certificat

Dans cet exercice, vous allez apprendre comment installer un certificat dans le magasin de certificats de Windows 10.

1. Ouvrez le certificat **VotreNom.crt** et cliquez sur **Installer ce certificat**.

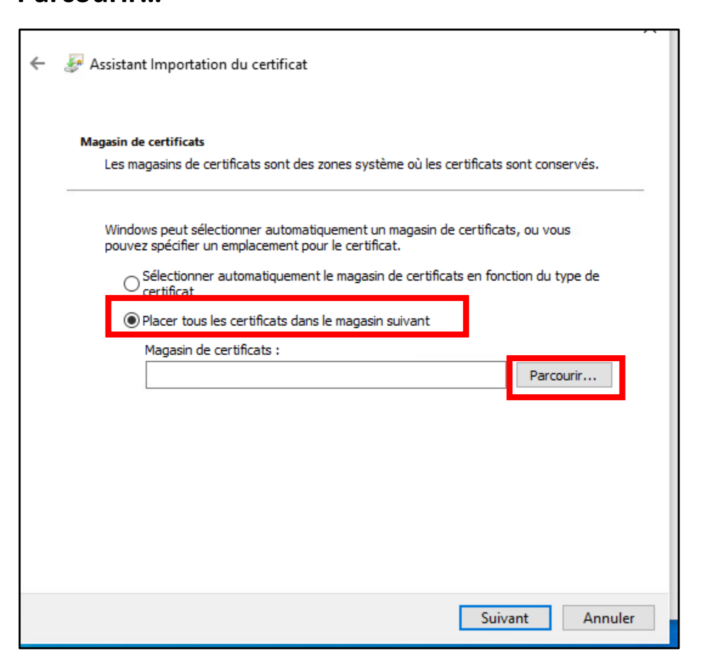


2. Dans la fenêtre **Assistant Importation du certificat**, sélectionnez **Ordinateur local**, puis cliquez sur **Suivant.**

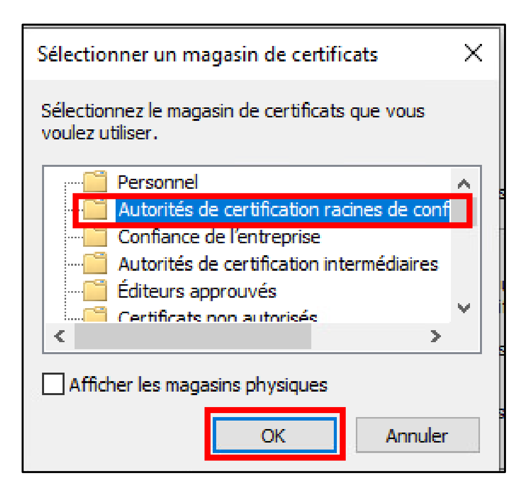


3. Cliquez sur **Oui** pour autoriser.

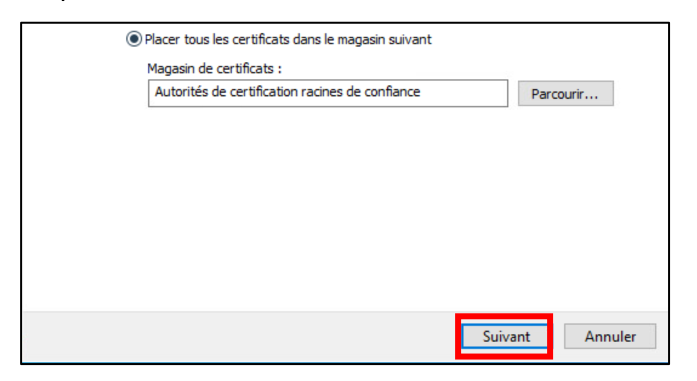
4. Sélectionnez **Placer tous les certificats dans le magasin suivant** puis cliquez sur **Parcourir…**



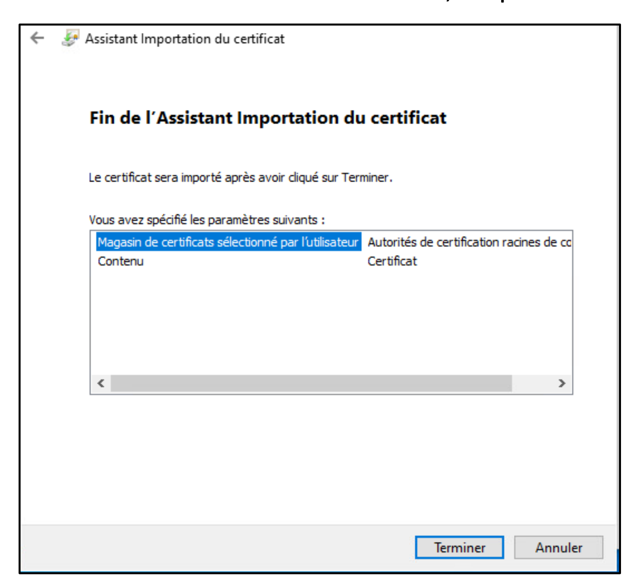
5. Sélectionnez **Autorité de certification racine de confiance** puis cliquez sur **OK.**



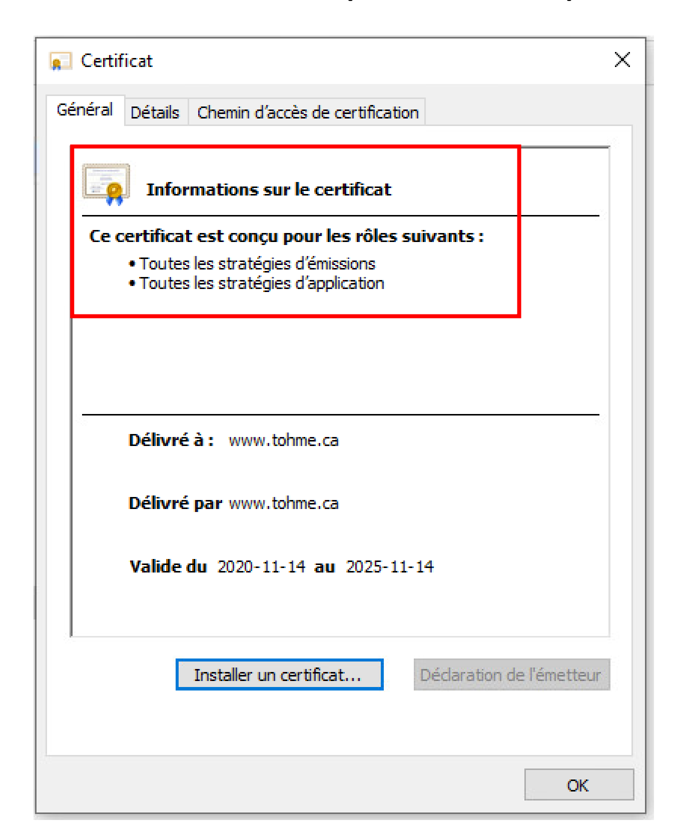
6. Cliquez sur **Suivant.**



7. Dans la fenêtre **Fin de l'Assistant**, cliquez sur **Terminer**, puis cliquez sur **OK.**



8. Fermez le certificat puis ouvrez le encore une fois. Vous allez trouver qu'il n'y a pas d'erreur, et **le certificat peut être utilisé pour chiffrer et signer les données**.



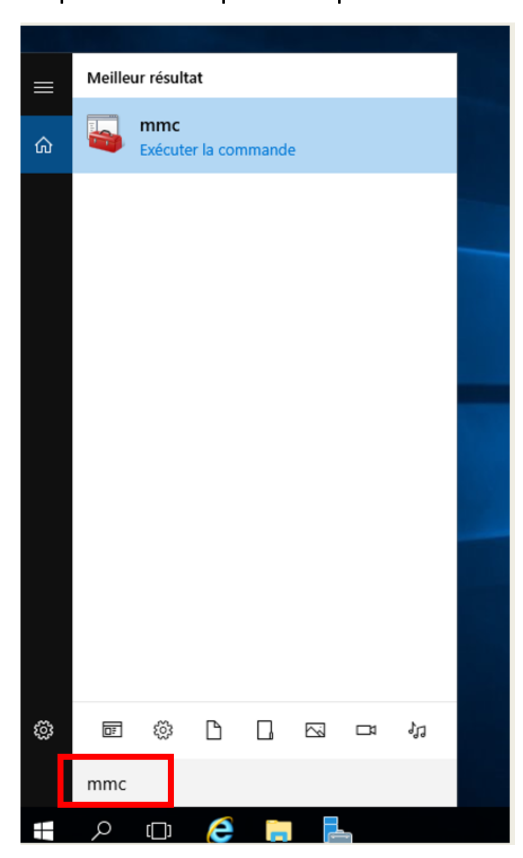
IMPORTANT 4 : Prenez une capture d'écran de ce certificat et mettez-la dans le doc Word.

9. Fermez **le certificat**.

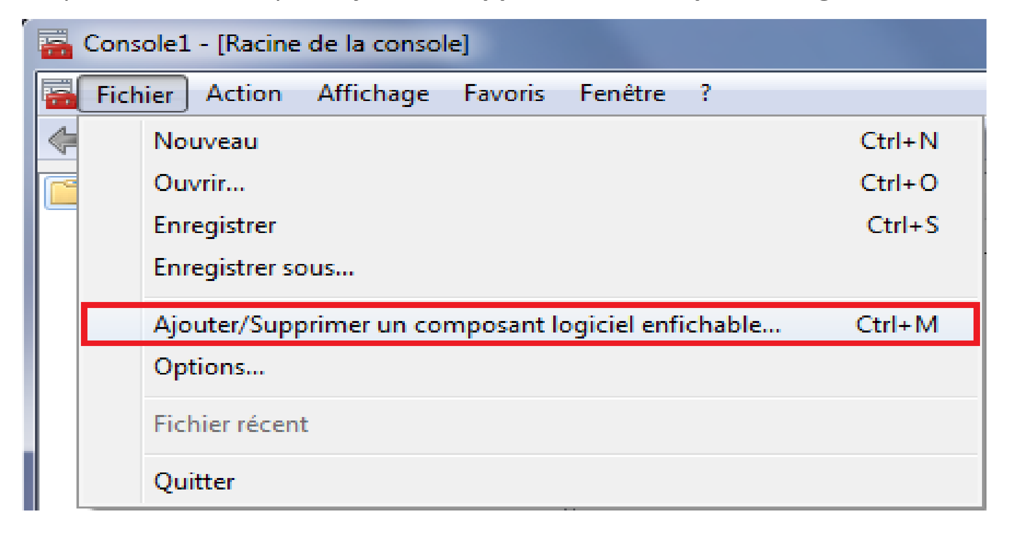
Exercice 5 – Magasin de certificats

Dans cet exercice, vous allez apprendre comment ouvrir le magasin de certificats de Windows 10

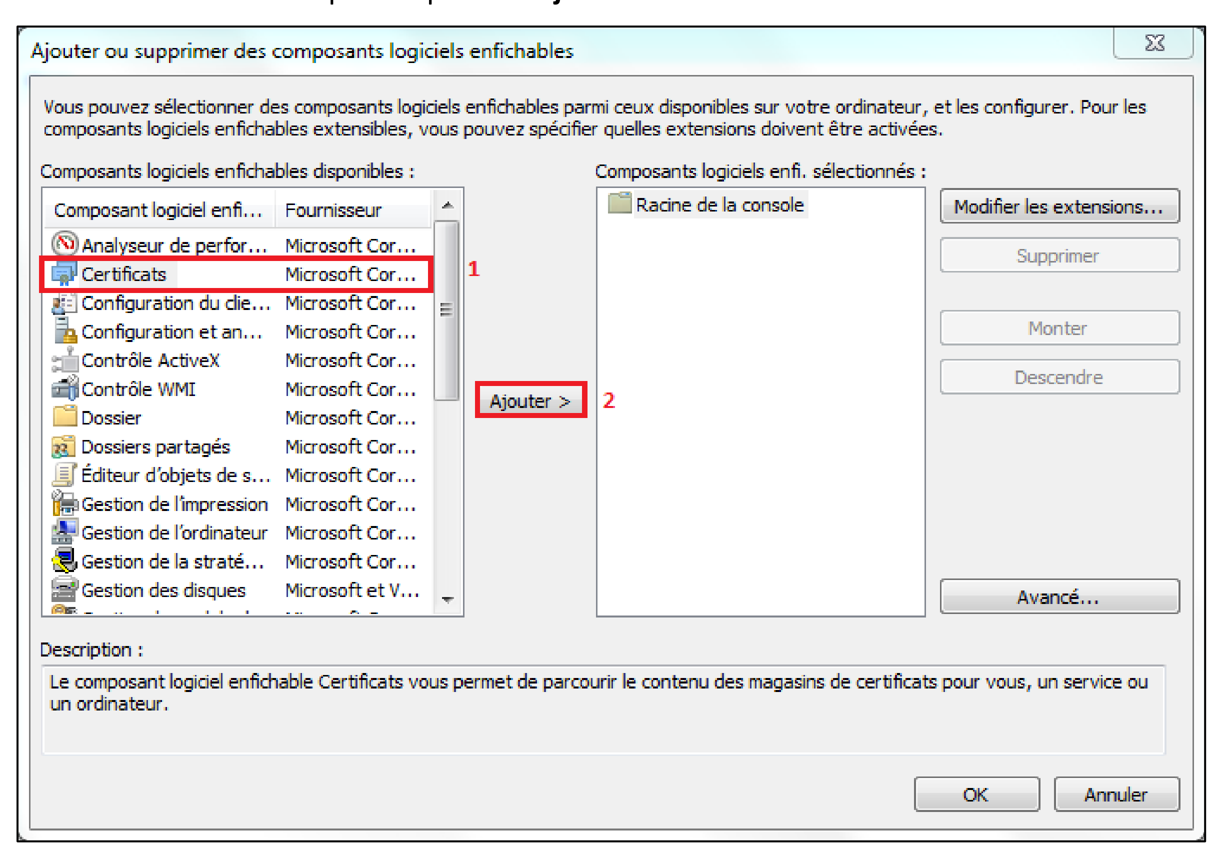
1. Tapez **mmc** dans le bouton rechercher, pour ouvrir la console de Microsoft, puis cliquez sur **Oui** pou accepter.



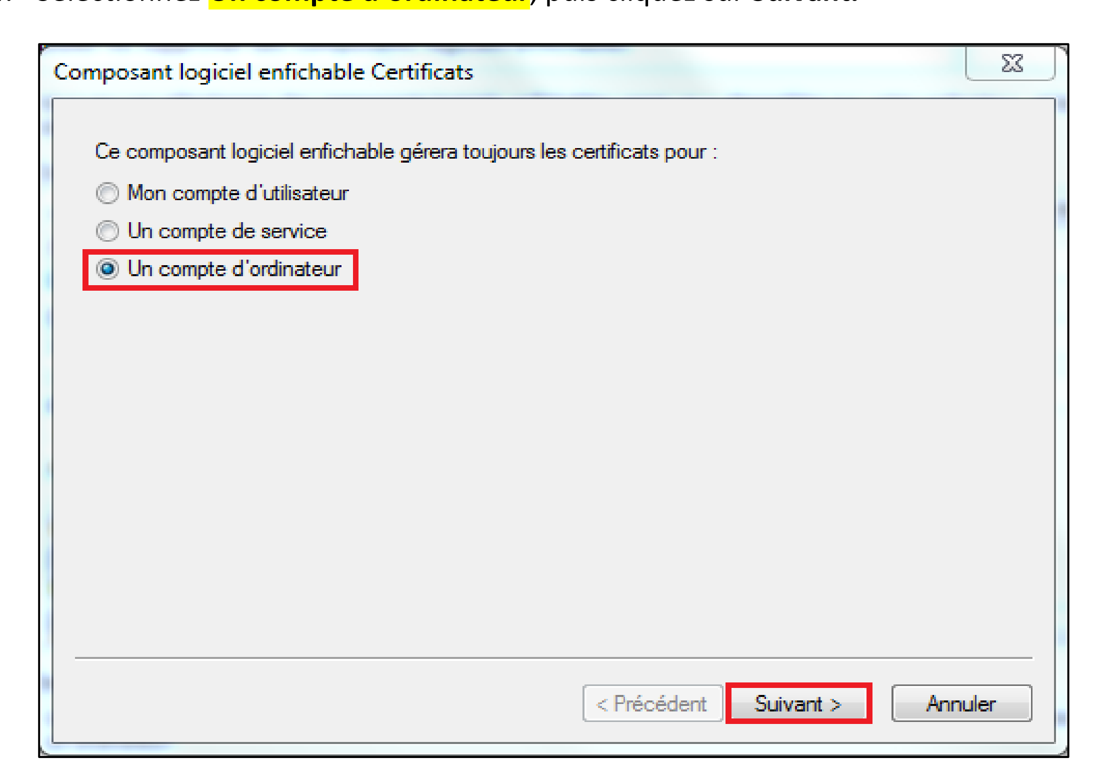
2. Cliquez sur **Fichier**, puis **Ajouter/Supprimer un composant logiciel enfichable**.



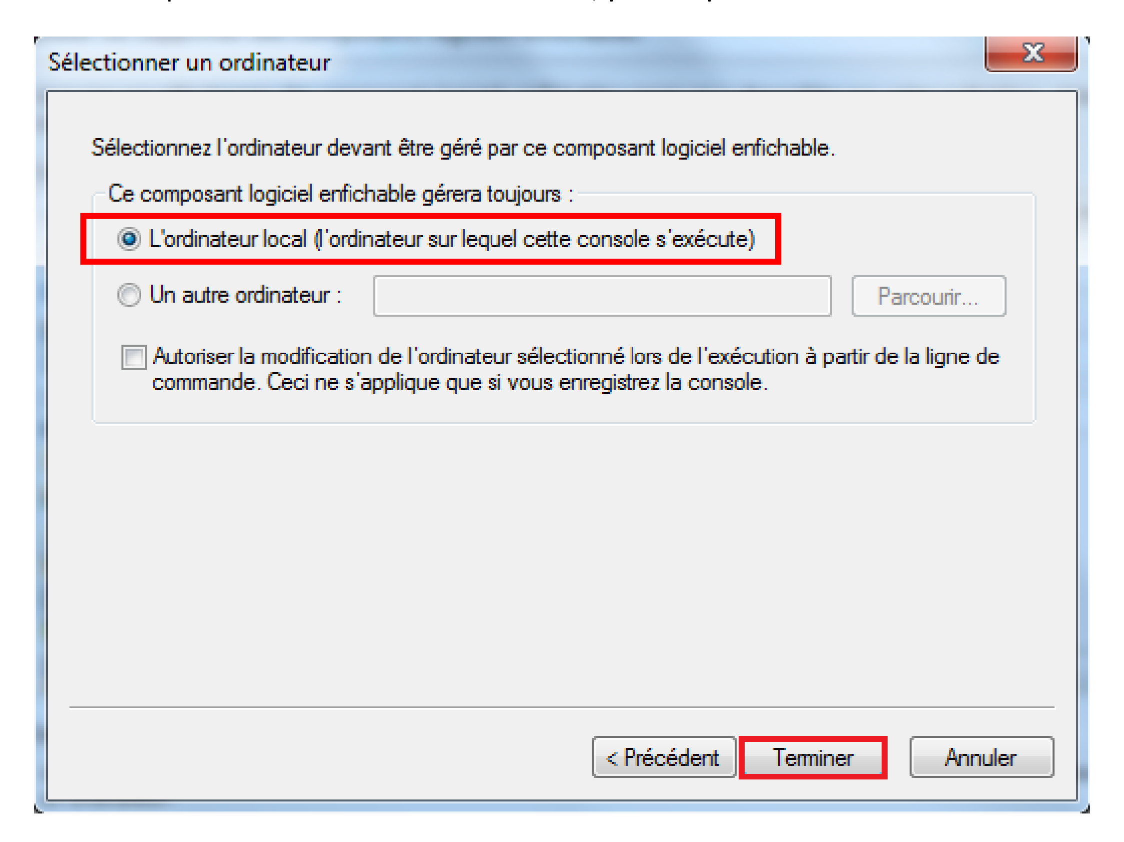
3. Sélectionnez **Certificats** puis cliquez sur **Ajouter.**



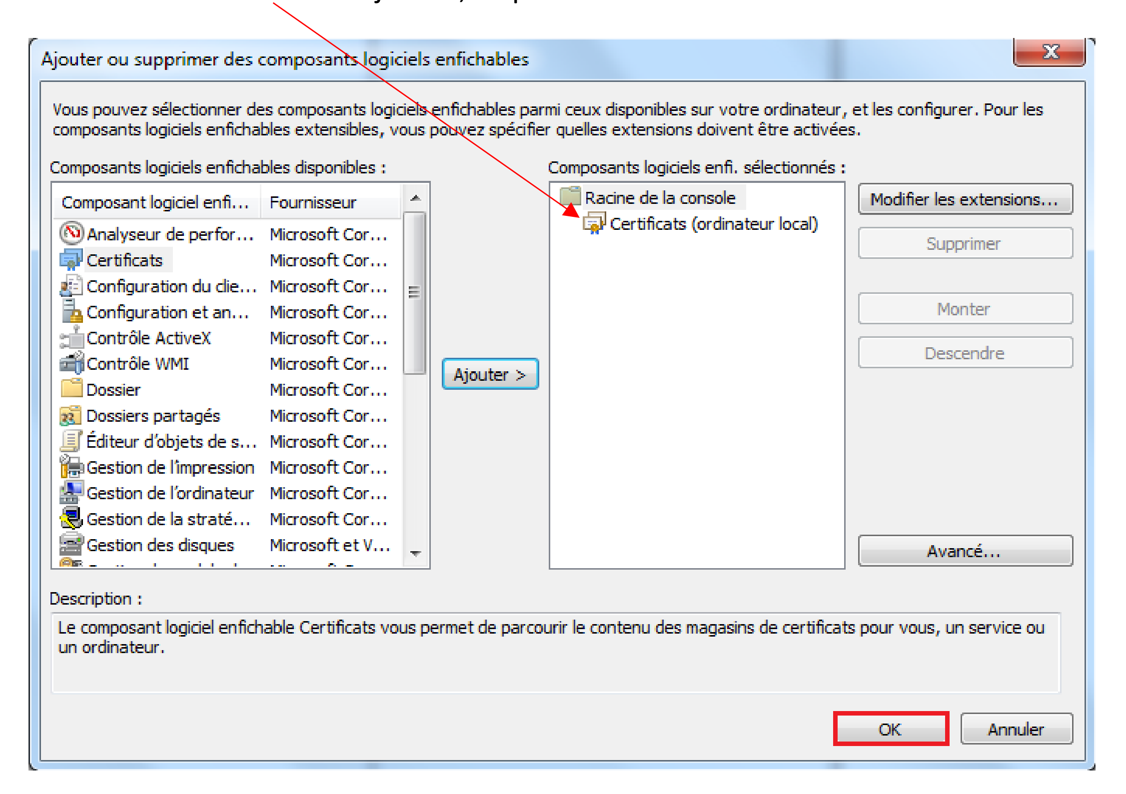
4. Sélectionnez **Un compte d'ordinateur**, puis cliquez sur **Suivant.**



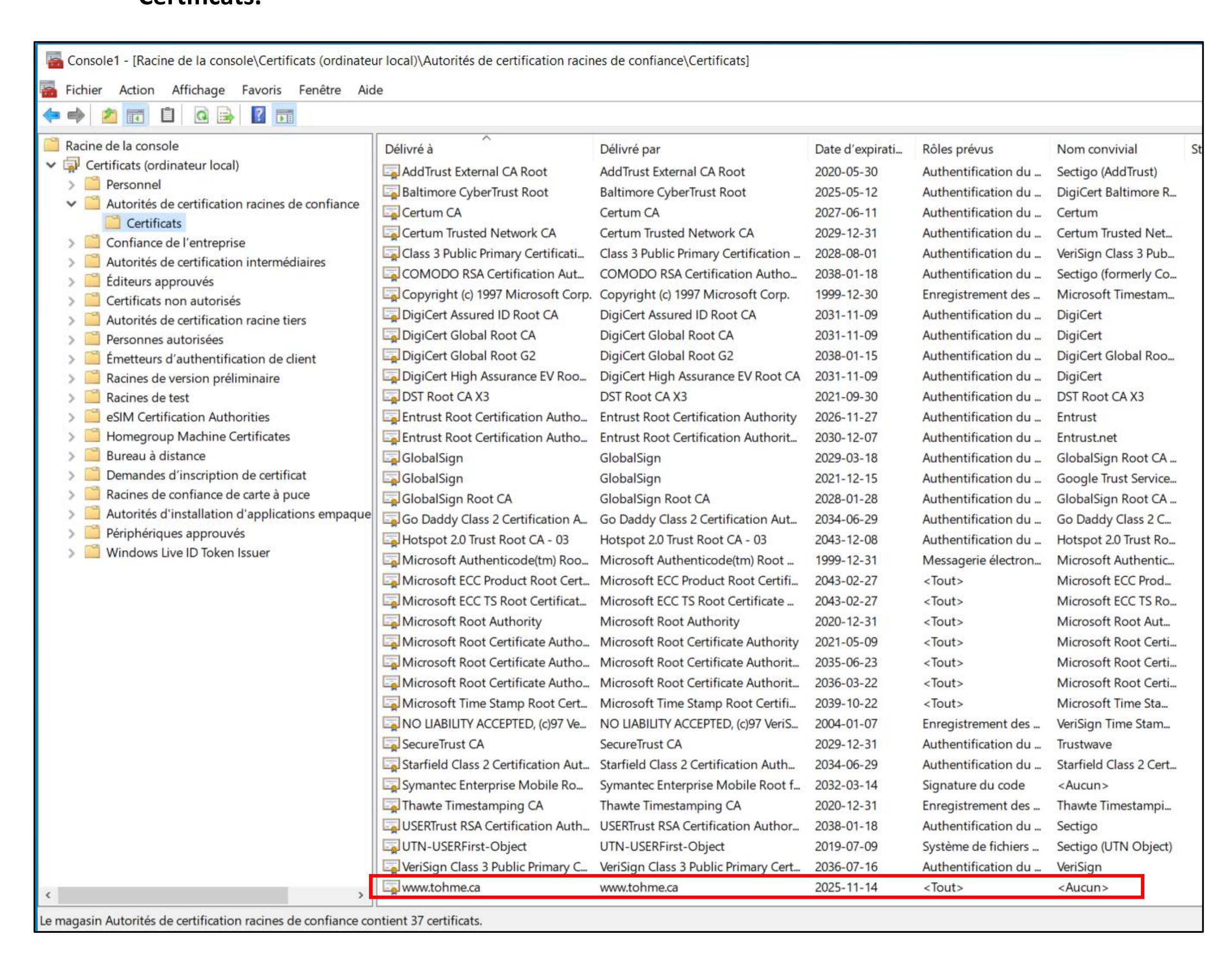
5. Gardez l'option: **L'ordinateur local...** coché, puis cliquez sur **Terminer**.



6. La console **Certificats** est ajoutée, cliquez sur **OK.**



7. Développez le dossier **Certificats (ordinateur local)**, puis développez le dossier **Autorités de certification racine de confiance**, ensuite cliquez sur le dossier **Certificats.**



8. Vous allez voir ici tous les serveurs d'autorité de certification autorisés par Windows 10, incluant ce que **vous avez installé dans l'exercice 4 précédente**.

IMPORTANT 5 : Prenez une capture d'écran de cette fenêtre et mettez-la dans le doc Word.

10. Fermez cette fenêtre, sans l'enregistrée.

11. Déconnectez-vous de Windows.